Normal cyclotomic schemes over a finite commutative ring

Sergei Evdokimov
Steklov Institute of Mathematics
at St. Petersburg
evdokim@pdmi.ras.ru

Ilia Ponomarenko
Steklov Institute of Mathematics
at St. Petersburg
inp@pdmi.ras.ru *

15.08.2006

Abstract

We study cyclotomic association schemes over a finite commutative ring R with identity. The main interest for us is to identify the normal cyclotomic schemes $\mathcal{C}$, i.e. those for which $\mathrm{Aut}(\mathcal{C}) \le A\Gamma L_1(R)$. The problem is reduced to the case when the ring R is local in which a necessary condition of normality in terms of the subgroup of $R^\times$ defining $\mathcal{C}$, is given. This condition is proved to be sufficient for a class of local rings including the Galois rings of odd characteristic.

1 Introduction

Let R be a finite commutative ring[1] and K a subgroup of its multiplicative group $R^\times$. Denote by $\mathrm{Rel}(K,R)$ the set of all binary relations on R of the form $\{(x,y) \in R \times R : y - x \in rK\}$, $r \in R$. Then the pair

$$\mathrm{Cyc}(K,R) = (R, \mathrm{Rel}(K,R)) \tag{1}$$

is an association scheme on R. We call it a *cyclotomic scheme over* R corresponding to the group K. Clearly, it is the scheme of 2-orbits of the group $\Gamma(K,R) = \{\gamma_{a,b} : a \in K, b \in R\}$ where $\gamma_{a,b}$ is the permutation of the set R taking x to $ax+b$. In particular, it is a Cayley scheme over the additive group R^+ of R (see Subsection 7.2) or a translation scheme in the sense of [1]. Moreover, the multiplications by elements of $R^\times$ are Cayley isomorphisms of this scheme.

Cyclotomic schemes over a field were introduced by P. Delsarte (1973) in connection with coding theory. In [7] it was proved that any such scheme is uniquely determined up to isomorphism by its 3-dimensional intersection numbers. Cyclotomic schemes over rings were introduced and studied in [3] within the framework of the duality theory for association schemes. We also mention paper [6] where cyclotomic schemes over Galois rings were used to construct amorphous association schemes. In the present paper we are interested in the automorphism groups of cyclotomic schemes.

*The work was supported by RFFI Grants 05-01-00899 and NSH-4329.2006.1.

[1] Throughout the paper all rings are supposed to have identity.

Historically, as the first result on the automorphism groups of cyclotomic schemes one should consider the well-known Burnside theorem on permutation groups of prime degree. In fact, this theorem completely determine the former groups for a prime field. In the case of an arbitrary finite field we have the following result which is the interpretation of an old number-theoretical result from [4] (see also [1, p.389]).

Theorem 1.1 *If $\mathcal{C}$ is a cyclotomic scheme over a finite field $\mathbb{F}$, then* $\mathrm{Aut}(\mathcal{C}) \le \mathrm{A\Gamma L}_1(\mathbb{F})$ *whenever* $\mathrm{rk}(\mathcal{C}) > 2$.■

For the cyclotomic schemes over the ring $\mathbb{Z}_n$ of integers modulo a positive integer n the result of such a kind is not true. Indeed, any such scheme being a Cayley scheme over a cyclic group $\mathbb{Z}_n^+$ can be treated up to language as an S-ring over the same group. In accordance with [8, 7] each such S-ring can be constructed from normal S-rings and S-rings of rank 2 by means of tensor products and generalized wreath products (or wedge products in terms of [8]). Here normal S-rings are exactly those coming from cyclotomic schemes $\mathcal{C}$ such that $\mathrm{Aut}(\mathcal{C}) \le \mathrm{A\Gamma L}_1(\mathbb{Z}_n) = \mathrm{AGL}_1(\mathbb{Z}_n)$. However, even among the S-rings corresponding to cyclotomic schemes there exist non-normal ones.

The above discussion leads to the following definition which is central for this paper.

Definition 1 *A cyclotomic scheme $\mathcal{C}$ over a finite commutative ring R is called normal if* $\mathrm{Aut}(\mathcal{C}) \le \mathrm{A\Gamma L}_1(R)$.

The goal of the paper is to identify normal cyclotomic schemes. Since any finite commutative ring is the direct product of local rings, the following theorem reduces the general case to the local one (and, moreover, gives some product formula for two-points stabilizers of the automorphism group). Below for $R = \prod_i R_i$ we use the following notation. For a cyclotomic scheme $\mathcal{C} = \mathrm{Cyc}(K, R)$ set $\mathcal{C}_i = \mathrm{Cyc}(K_i, R_i)$ where K_i is defined from the equality $\varphi_i(K_i) = K \cap \varphi_i(R_i^\times)$ with φ_i being the monomorphism of $R_i^\times$ to $R^\times$ such that the jth component of $\varphi_i(x)$ equals x for $j = i$, and equals 1_{R_j} for $j \ne i$.

Theorem 1.2 *Let $R = \prod_i R_i$ be a finite commutative ring and $\mathcal{C}$ a cyclotomic scheme over R. Then*

$$\mathrm{Aut}(\mathcal{C})_{u,v} = \prod_i \mathrm{Aut}(\mathcal{C}_i)_{u_i,v_i} \tag{2}$$

where $u = 0_R$, $v = 1_R$ and $u_i = 0_{R_i}$, $v_i = 1_{R_i}$ for all i. In particular, $\mathcal{C}$ is normal iff the scheme $\mathcal{C}_i$ is normal for all i.

The following theorem gives a necessary condition for a cyclotomic scheme over a local ring to be normal. We do not know any example when this condition is not sufficient. Below we set $I_0 = \{x \in \mathrm{rad}(R) : x\,\mathrm{rad}(R) = \{0\}\}$.

Theorem 1.3 *Let a cyclotomic scheme* $\mathrm{Cyc}(K, R)$ *over a finite local commutative ring R be normal. Suppose that $K = K + I$ for some ideal I of R. Then $I = \{0\}$ unless $q = 2$ where q is the order of the residue field of R. Moreover, if $q = 2$, then $I \subset I_0$.*

Let R be a local commutative ring. Given a group $K \le R^\times$ denote by $\mathcal{I}_K$ the set of all ideals I of R such that $K + I = K$ or, equivalently, $1 + I \subset K$. It is convenient for us to formulate the following definition.

Definition 2 *A group $K \le R^\times$ is called pure if the condition $I \in \mathcal{I}_K$ implies that $I = \{0\}$.*

If R is a field, then obviously any subgroup of $R^\times$ is pure. Besides, Theorem 1.3 implies that for $q > 2$ the group K is pure whenever the scheme $\mathrm{Cyc}(K, R)$ is normal. It turns out that for the Galois rings of odd characteristic other than fields this necessary condition of normality is also sufficient (as for the definition of a Galois ring see Section 2).

Theorem 1.4 *Let R be a Galois ring of odd characteristic other than a field. Then the scheme $\mathrm{Cyc}(K, R)$ is normal iff the group K is pure.*

Let $R = \mathrm{GR}(p^d, r)$ be a Galois ring of characteristic p^d with the residue field of cardinality $q = p^r$ where p is a prime. If $d > 1$ and $p > 2$ (the case of Theorem 1.4), then it is easy to see that a group $K \le R^\times$ is pure iff it does not contain the group $1 + p^{d-1}R$. On the other hand, if $d = 1$, i.e. $R = \mathbb{F}$ is a field of cardinality q, then the equality $\mathrm{rk}(\mathcal{C}) = 2$ implies that $\mathrm{Aut}(\mathcal{C}) = \mathrm{Sym}(\mathbb{F})$. Besides, $\mathrm{Sym}(\mathbb{F}) \le \mathrm{A\Gamma L}_1(\mathbb{F})$ iff $q \le 4$. Thus after combining Theorems 1.4 and 1.1 we come to the following statement.

Theorem 1.5 *Let $R = \mathrm{GR}(p^d, r)$ with $p > 2$. Then a cyclotomic scheme $\mathrm{Cyc}(K, R)$ is normal exactly in one of the following cases:*

(1) *$d = 1$ and either $(p, r) = (3, 1)$ or $K \ne R^\times$,*

(2) *$d > 1$ and $K \not\ge 1 + p^{d-1}R$.* ∎

One of the ideas to prove the sufficiency in Theorem 1.4 is to develop a reduction technique for cyclotomic schemes over an arbitrary local ring R. For an ideal I of R the scheme $\mathrm{Cyc}(\pi_I(K), R/I)$ where $\pi_I : R \to R/I$ is the natural epimorphism, can be treated as a factor-scheme of the scheme $\mathrm{Cyc}(K, R)$ (see Subsection 2.2). This simple observation is used in the proof of Theorem 6.1 a straightforward consequence of which is the following reduction statement. Below we set $\pi_0 = \pi_{I_0}$.

Theorem 1.6 *Let R be a finite local commutative ring, $\mathcal{C} = \mathrm{Cyc}(K, R)$ where $K \le R^\times$ is a pure group, and $\mathcal{C}' = \mathrm{Cyc}(K', R')$ where $K' = \pi_0(K)$ and $R' = R/I_0$. Then the scheme $\mathcal{C}$ is normal whenever so is the scheme $\mathcal{C}'$.* ∎

Unfortunately, in the general case the group K' is not pure (even if R is a Galois ring of even characteristic). So Theorem 1.6 cannot be used for a direct inductive proof of the normality of the scheme $\mathcal{C}$. However, if R is a Galois ring of odd characteristic, then this is true and Theorem 1.4 is reduced to the case $\mathrm{rad}(R)^2 = \{0\}$. Thus, due to Theorem 1.1 it suffices to prove the following statement which is a special case of Theorem 6.4.

Theorem 1.7 *Let R be a finite local commutative ring other than a field for which $\mathrm{rad}(R)^2 = \{0\}$. Then the scheme $\mathrm{Cyc}(K, R)$ is normal whenever the group K is pure.* ∎

Theorems 6.1 and 6.4 which are the origins of Theorems 1.6 and 1.7 are proved by using the S-ring technique. Namely, for a cyclotomic scheme $\mathcal{C}$ over R together with the ordinary (addition) S-ring over R^+ corresponding to $\mathcal{C}$ we consider its *multiplication* S-ring $\mathcal{A}$ over $R^\times$ (see Section 4). Everything is reduced to the case of a pure group $K \le \mathcal{T}\mathcal{U}_0$ where $\mathcal{T}$ is the Teichmüller subgroup of $R^\times$ and $\mathcal{U}_0 = 1 + I_0$. Then the group $\mathrm{Aut}(\mathcal{C})_{u,v}$

acts faithfully on $R^\times$ and the image of this action equals $\mathrm{Aut}(\mathcal{A})$. Moreover, in this case the S-ring $\mathcal{A}$ contains the groups $\mathcal{T}$ and $\mathcal{U} = 1 + \mathrm{rad}(R)$, and becomes trivial after adding to it the cosets by any of these groups (Section 5). This enables us to prove that the group $\mathrm{Aut}(\mathcal{C})$ normalizes the group $\mathrm{AGL}_1(R)$ (Theorems 4.3 and 7.2). The latter means that $\mathrm{Aut}(\mathcal{C}) \le \mathrm{A\Gamma L}_1(R)$ (Lemma 2.1), i.e. the scheme $\mathcal{C}$ is normal.

In fact, the developed technique permits us to obtain the following sufficient condition of normality for an arbitrary finite local commutative ring R: the scheme $\mathrm{Cyc}(K, R)$ is normal whenever the group K is strongly pure (Theorem 6.2). (Here we call a group $K \le R^\times$ *strongly pure* if it is pure and the group $\pi_0(K)$ is strongly pure unless R is a field.) It should be noted that this condition is not necessary: one can prove that the cyclotomic scheme corresponding to the non-strongly pure group K from the example in the beginning of Subsection 6.2 is normal.

In some cases one can say a little bit more on the automorphism group of a normal cyclotomic scheme $\mathcal{C} = \mathrm{Cyc}(K, R)$ where R is a finite local commutative ring. For instance, if $K \le \mathcal{T}$ and R is not a field, then

$$\mathrm{Aut}(\mathcal{C}) \le \mathrm{AGL}_1(R)$$

(statement (1) of Theorem 6.5). This inclusion remains true also in some other cases. In particular, this is so if the group K is strongly pure, and either $K \le \mathcal{U}$ or the residue filed $\mathbb{F}$ of R is prime (statements (2) and (3) of Theorem 6.5). The reason of this is that in both cases the natural mapping

$$\mathrm{Aut}_{\mathcal{C}}(R) \to \mathrm{Aut}_{\mathcal{C}}(\mathbb{F})$$

is a monomorphism and the group $\mathrm{Aut}_{\mathcal{C}}(\mathbb{F})$ is trivial where by definition $\mathrm{Aut}_{\mathcal{C}}(R)$ (resp. $\mathrm{Aut}_{\mathcal{C}}(\mathbb{F})$) consists of all automorphisms of R (resp. $\mathbb{F}$) that are automorphisms of $\mathcal{C}$ (resp. the factor-scheme of $\mathcal{C}$ on $\mathbb{F}$) (see Theorem 6.2). It should be noted that generally the kernel of the quotient homomorphism $\mathrm{Aut}(R) \to \mathrm{Aut}(\mathbb{F})$ is not trivial. For instance, for $R = \mathbb{F}[X]/(X^2)$ the group $\mathrm{Aut}(R)$ is isomorphic to the semidirect product of $R^\times$ by $\mathrm{Aut}(\mathbb{F})$ (indeed, the mapping $a + b\pi \mapsto a^\sigma + b^\sigma \alpha \pi$ where $a, b \in \mathbb{F}$ and $\pi = X \mod X^2$, is an automorphism of R for any $\sigma \in \mathrm{Aut}(\mathbb{F})$ and $\alpha \in R^\times$).

All undefined terms and results concerning permutation groups can be found in [10, 11, 2]. To make the paper self-contained we cite the background on schemes and Schur rings in Section 7. All necessary properties of finite rings and cyclotomic schemes can be found in Section 2. The proofs of Theorems 1.2 and 1.3 are contained in Section 3, they are based on the ideas of [7] where the case $R = \mathbb{Z}_n$ was treated. The multiplication S-ring of a cyclotomic scheme is introduced and studied in Sections 4 and 5. Section 6 contains the proofs of Theorems 6.1, 6.2, and 1.4.

Notations. As usual by $\mathbb{Z}$ we denote the ring of integers.

For a ring R with identity we denote by R^+, $R^\times$ and $\mathrm{rad}(R)$ the additive and multiplicative groups of R and the radical of R respectively.

Given groups $A \le R^\times$ and $B \le R^+$ with $AB = B$ we denote by $\Gamma(A, B)$ the group $\{\gamma_{a,b} : \ a \in A, \ b \in B\}$ where $\gamma_{a,b}$ is the permutation of R taking x to $ax + b$. We omit B whenever $B = \{0\}$.

The group of all permutations of V is denoted by $\mathrm{Sym}(V)$.

Each permutation $f \in \mathrm{Sym}(V)$ ($v \mapsto v^f$) naturally defines a permutation $R \mapsto R^f$ of the set of all relations on V. For an equivalence relation E on a set $X \subset V$ such that $E^f = E$, the permutation f induces a permutation $f^{X/E} \in \mathrm{Sym}(X/E)$. If all classes of E are singletons, the set X/E is identified with X.

For a group G the permutation group on the set G defined by the right multiplications is denoted by G_{right}.

For $\Gamma \le \mathrm{Sym}(V)$ and $X_1, \dots, X_s \subset V$ we set $\Gamma_{X_1,\dots,X_s} = \{\gamma \in \Gamma : X_i^\gamma = X_i \text{ for all } i\}$. If $X_i = \{v_i\}$, the brackets are omitted. If the X_i's are the classes of an equivalence E on V, we set $\Gamma_E = \Gamma_{X_1,\dots,X_s}$.

2 Finite commutative rings and cyclotomic schemes

2.1 Finite rings. It is well known (see e.g. [5, Theorem 6.2]) that any finite commutative ring is the direct product of local rings. Let R be a finite local commutative ring. Then $R = \mathrm{rad}(R) \cup R^\times$, the ideal $\mathrm{rad}(R)$ is maximal and the characteristic of R is a power of the characteristic of its residue field $\mathbb{F} = R/\mathrm{rad}(R)$. Moreover,

$$R^\times = \mathcal{T} \times \mathcal{U} \tag{3}$$

where $\mathcal{T}$ is the Teichmüller group and $\mathcal{U}$ is the group of principal units. The groups $\mathcal{T}$ and $\mathcal{U} = 1 + \mathrm{rad}(R)$ are a cyclic group of order $q-1$ and an abelian p-group respectively where q and p are the order and the characteristic of $\mathbb{F}$.

Let $I \subset \mathrm{rad}(R)$ be an ideal of R. Then the quotient ring R/I is local and $(R/I)^\times = \pi_I(R^\times)$ where $\pi_I : R \to R/I$ is the natural epimorphism. Besides, the set $1 + I$ is a subgroup of $\mathcal{U}$. In particular, if $I \subset I_0$ then the mapping $r \mapsto 1 + r$ induces an isomorphism of the additive group of I onto $1 + I$. Below we set $\mathcal{U}_0 = 1 + I_0$.

The local ring R is called *Galois* if $\mathrm{rad}(R) = pR$.[2] Given positive integers n, r there exists a unique up to isomorphism Galois ring of characteristic p^n with $q = p^r$; it is denoted by $\mathrm{GR}(p^n, r)$. We observe that $\mathrm{GR}(p, r)$ is a field of order p^r and $\mathrm{GR}(p^n, 1) \cong \mathbb{Z}_{p^n}$. Each proper ideal of the Galois ring $\mathrm{GR}(p^n, r) = R$ is of the form $p^i R$, $i = 1, \dots, n$, and the quotient ring is isomorphic to $\mathrm{GR}(p^i, r)$. We also note that the homomorphism $\mathrm{Aut}(R) \to \mathrm{Aut}(\mathbb{F})$ induced by the epimorphism $\pi_{\mathrm{rad}(R)}$ is in fact an isomorphism (see [9]).

Generally, the structure of the group $\mathrm{Aut}(R)$ (even in the local case) is unclear. Below we give a sufficient condition for a permutation of R to belong to this group.

Lemma 2.1 *Let R be a commutative ring and let a group $K \le R^\times$ generate R^+. Suppose that $\gamma \in \mathrm{Sym}(R)$ is such that*

$$0^\gamma = 0, \quad 1^\gamma = 1, \quad \gamma^{-1}\Gamma(K, R)\gamma = \Gamma(K, R).$$

Then $\gamma \in \mathrm{Aut}(R)$.

Proof. From the condition $\gamma^{-1}\Gamma(K, R)\gamma = \Gamma(K, R)$ it follows that given $(a, b) \in K \times R$ there exists $(a_\gamma, b_\gamma) \in K \times R$ such that $\gamma^{-1}\gamma_{a,b}\gamma = \gamma_{a_\gamma, b_\gamma}$, or, equivalently,

$$(ax^{\gamma^{-1}} + b)^\gamma = a_\gamma x + b_\gamma, \quad x \in R. \tag{4}$$

[2] This is one of the equivalent definitions given in [5].

Since γ leaves fixed both 0 and 1, for $x = 0$ this implies that $b_\gamma = b^\gamma$ for all $b \in R$, whereas for $(x, b) = (1, 0)$ this implies that $a_\gamma = a^\gamma$ for all $a \in K$. Now, for $a = 1$ and for $b = 0$ the equality (4) gives

$$(x + b)^\gamma = x^\gamma + b^\gamma, \quad (x, b) \in R \times R, \quad \text{and} \quad (ax)^\gamma = a^\gamma x^\gamma, \quad (a, x) \in K \times R \qquad (5)$$

respectively. In particular, $\gamma \in \mathrm{Aut}(R^+)$ and consequently (since K generates R^+) the second equality holds for all $a \in R$. Thus, $\gamma \in \mathrm{Aut}(R)$.■

Lemma 2.1 will be applied in Section 6 to a local ring R and $K = R^\times$. In this case $\langle K\rangle = R^+$ because any element of $\mathrm{rad}(R) = R \setminus R^\times$ is the difference of two units. One more application is given by the following statement where $s = \gamma_{-1,1}$ is the involution taking x to $-x + 1$.

Corollary 2.2 *Let $\mathbb{F}$ be a field and $\gamma \in \mathrm{Sym}(\mathbb{F})$ a permutation leaving fixed both 0 and 1. Suppose that γ normalizes both the groups $\Gamma(\mathbb{F}^\times)$ and $s\Gamma(\mathbb{F}^\times)s$. Then $\gamma \in \mathrm{Aut}(\mathbb{F})$.*

Proof. A straightforward computation shows that $\gamma_{a^{-1},0} s \gamma_{a,0} s = \gamma_{1,1-a}$ for all $a \in \mathbb{F}^\times$. Then assuming (without loss of generality) that $|\mathbb{F}| > 2$ we see that the group $\langle \Gamma(\mathbb{F}^\times), s\Gamma(\mathbb{F}^\times)s\rangle$ contains the group $\Gamma(1, \mathbb{F}^+)$ and hence equals $\Gamma(\mathbb{F}^\times, \mathbb{F}^+)$. Since obviously $\langle \mathbb{F}^\times\rangle = \mathbb{F}$, we are done by Lemma 2.1 with $R = \mathbb{F}$ and $K = \mathbb{F}^\times$.■

2.2 Cyclotomic schemes. Let $\mathcal{C} = \mathrm{Cyc}(K, R)$ be a cyclotomic scheme over a finite commutative ring R (see (1)). Since obviously each relation from $\mathrm{Rel}(K, R)$ is R^+_{right}-invariant, $\mathcal{C}$ is a Cayley scheme over the group R^+. The corresponding S-ring is called the *addition S-ring* of $\mathcal{C}$. Each basic set of it is of the form rK where $r \in R$. It follows that any ideal I of R is an $\mathcal{A}$-subgroup (indeed, $I = \bigcup_{r\in I} rK$). So due to the bijection between the sets $\mathcal{H}(\mathcal{A})$ and $\mathcal{E}(\mathcal{C})$ (see Subsection 7.2) we have the following statement.

Lemma 2.3 *For any ideal I of R the binary relation*

$$E(I) = \bigcup_{X\in R/I} X \times X$$

belongs to the set $\mathcal{E}(\mathcal{C})$. In particular, the equivalence $E(I)$ is $\mathrm{Aut}(\mathcal{C})$-invariant.■

Since the set $\mathrm{Rel}(K, R)$ is obviously $\mathrm{AGL}_1(R)$-invariant and the stabilizer of $u = 0$ in $\mathrm{AGL}_1(R)$ equals $\mathrm{GL}_1(R)$ we have

$$\mathrm{AGL}_1(R) \le \mathrm{Iso}(\mathcal{C}), \quad \mathrm{GL}_1(R) \le \mathrm{Iso}(\mathcal{C}_u) \qquad (6)$$

where $\mathcal{C}_u$ is the u-extension of $\mathcal{C}$ (see Subsection 7.1). The following easy statement gives a simple criterion of normality.

Lemma 2.4 *The scheme $\mathcal{C}$ is normal iff $\mathrm{Aut}(\mathcal{C})_{u,v} \le \mathrm{Aut}(R)$ where $u = 0$ and $v = 1$.*

Proof. The necessity follows from the obvious equality $\mathrm{A\Gamma L}(R)_{u,v} = \mathrm{Aut}(R)$. Conversely, by the orbit-stabilizer property [2, Theorem 1.4A] we have

$$[\mathrm{Aut}(\mathcal{C}) : \mathrm{Aut}(\mathcal{C})_{u,v}] = |R||K| = |\Gamma(K, R)|.$$

Since $\Gamma(K,R) \le \mathrm{Aut}(\mathcal{C})$, we conclude that $\mathrm{Aut}(\mathcal{C}) = \mathrm{Aut}(\mathcal{C})_{u,v}\Gamma(K,R)$ and the sufficiency follows.∎

Now let the ring R be local and $I \subset \mathrm{rad}(R)$ an ideal of R. Then $R/E(I) = R/I$, the equivalence relation $E(I)$ is $\Gamma(K,R)$-invariant and $\Gamma(K,R)^{R/E(I)} = \Gamma(\pi_I(K), R/I)$. This implies that

$$\mathrm{Cyc}(K,R)_{R/E(I)} = \mathrm{Cyc}(\pi_I(K), R/I), \tag{7}$$

i.e. the factor-scheme of $\mathcal{C}$ modulo the equivalence $E(I)$ can naturally be treated as a cyclotomic scheme over the ring R/I.

The following theorem on cyclotomic schemes with pure groups (see Definition 2) will be used in Section 6.

Theorem 2.5 *Let $\mathcal{C} = \mathrm{Cyc}(K,R)$ be a cyclotomic scheme over a local commutative ring R. If the group K is pure, then*

$$\mathcal{C}_{E_0} \ge \mathrm{Cyc}(U_0, R)$$

where $U_0 = K \cap \mathcal{U}_0$ and $E_0 = E(I_0)$.

Proof. First we prove that if $S \in \mathrm{Rel}(K,R)$ and $S_0 \in \mathrm{Rel}(U_0,R)$ are the relations corresponding to sets xK and xU_0 respectively, then

$$S \cap ((a+I_0)\times(b+I_0)) = S_0 \cap ((a+I_0)\times(b+I_0)), \qquad a,b \in R, \tag{8}$$

whenever $x \in R^\times$ and the right-hand side is nonempty. To do this let (y,z) belong to the left-hand side. Then $z-y \in (xK)\cap(b-a+I_0)$. On the other hand, due to the assumption there exists (y_0,z_0) belonging to the right-hand side. Then $z_0 - y_0 \in (xU_0)\cap(b-a+I_0)$. Thus, $(z-y)/(z_0-y_0) \in K \cap (1+I_0) = U_0$ and hence $z-y$ belongs to the right-hand side. The converse inclusion is obvious.

Denote by $\mathcal{M}$ the set of all relations from $\mathrm{Rel}(U_0,R)$ corresponding to the sets xU_0 with $x \in R^\times$. Then from (8) it follows that $\mathcal{M} \subset \mathcal{R}^*(\mathcal{C}_{E_0})$ and consequently $[\mathcal{M}] \le \mathcal{C}_{E_0}$. Thus it suffices to verify that $[\mathcal{M}] = \mathcal{C}_{E_0}$, or, equivalently, that the addition S-ring $\mathcal{A}$ of the scheme $\mathrm{Cyc}(U_0,R)$ is generated (as S-ring) by the sets xU_0, $x \in R^\times$. To do this we prove that

$$xU_0 = \bigcap_{t\in\mathcal{T}}((x-t)U_0 + tU_0), \quad x \in \mathrm{rad}(R). \tag{9}$$

Obviously, the left-hand side of (9) is contained in the right-hand side. Conversely, let $t \in \mathcal{T}$ and $x \in \mathrm{rad}(R)$. Then since $U_0 = 1+H$ and $xH = \{0\}$ where H is a subgroup of the group I_0, we have

$$(x-t)U_0 + tU_0 = (x-t)(1+H) + t(1+H) = x - t + tH + t + tH = x + tH.$$

It follows that if y belongs to the right-hand side of (9), then $y \in x + tH$ for all $t \in \mathcal{T}$. On the other hand, $\bigcap_{t\in\mathcal{T}} tH = \{0\}$ by the purity of U_0. Thus, $y = x$ and we are done.∎

3 Proof of Theorems 1.2 and 1.3

3.1 Proof of Theorem 1.2. Set $\Gamma = \mathrm{Aut}(\mathcal{C})$ and $\Gamma_i = \mathrm{Aut}(\mathcal{C}_i)$. To prove equality (2) first we verify that $\prod_i (\Gamma_i)_{u_i,v_i} \le \Gamma_{u,v}$. To this end we observe that from the obvious inclusion $\prod_i K_i \le K$ it follows that

$$\prod_i \Gamma(K_i, R_i) \le \Gamma(K, R).$$

So $\bigotimes_i \mathcal{C}_i \ge \mathcal{C}$ and hence $\prod_i \Gamma_i \le \Gamma$. Since obviously $\prod_i (\Gamma_i)_{u_i,v_i} = (\prod_i \Gamma_i)_{u,v}$, we are done. To prove the converse inclusion we observe that from Lemma 2.3 with $I = R_i$ it follows that R_i is a Γ_u-invariant set for all i. For $\gamma \in \Gamma_u$ denote by γ_i the restriction of γ to R_i. Then given an element $x = (\dots, x_i, \dots)$ of $R = \prod_i R_i$ we have

$$x^\gamma = (\dots, x_i^{\gamma_i}, \dots). \tag{10}$$

Indeed, by Lemma 2.3 with $I = \prod_{j \ne i} R_j$ the equivalence $E(I)$ is Γ_u-invariant. On the other hand, obviously each class of this equivalence contains a unique element of R_i. Thus, the ith component of x^γ equals $x_i^{\gamma_i}$ by the definition of γ_i. Since $\Gamma_{u,v,R_i,1+R_i} = \Gamma_{u,v}$, from (10) it follows that

$$\Gamma_{u,v} \le \prod_i (\Gamma_{u,v})^{R_i} = \prod_i (\Gamma_{u,v,R_i,1+R_i})^{R_i} \le \prod_i ((\Gamma_{R_i,1+R_i})^{R_i})_{u_i,v_i}.$$

Thus the inclusion $\prod_i (\Gamma_i)_{u_i,v_i} \ge \Gamma_{u,v}$ and hence equality (2) are easy consequences of Lemma 3.1 below. Indeed, since the groups Γ_i and $\Gamma(K_i, R_i)$ are 2-equivalent and the group Γ_i is 2-closed, it follows that $(\Gamma_{R_i,1+R_i})^{R_i} \le \Gamma_i$.

Lemma 3.1 *For any i the groups $(\Gamma_{R_i,1+R_i})^{R_i}$ and $\Gamma(K_i, R_i)$ are 2-equivalent.*

Proof. Set $X = R_i$ and $Y = 1 + R_i$. Since $\Gamma(K_i, R) \le \Gamma$ and $\Gamma(K_i, R_i) = (\Gamma(K_i, R)_{X,Y})^X$, it follows that $\Gamma(K_i, R_i) \le \Delta^X$ where $\Delta = \Gamma_{X,Y}$. So to prove the required statement it suffices to verify that each 2-orbit of the group Δ^X is contained in some 2-orbit of the group $\Gamma(K_i, R_i)$, or equivalently that each orbit of the group $(\Delta^X)_{u_i} = (\Delta_u)^X$ is contained in some orbit of the group $\Gamma(K_i, R_i)_{u_i} = K_i$ (here we made used of the fact that the group Δ^X contains a transitive subgroup $\Gamma(1, R_i)$). However, each orbit of the group $(\Delta_u)^X$ obviously meets some orbit of the group K_i. So we only have to check that the latter orbit is Δ_u-invariant. To do this we need the following statement.

Lemma 3.2 *For any i and for any $a, r \in R$ with $r_j \in R_j^\times$ for all $j \ne i$, we have*

$$(a + rK) \cap R_i = a_i + r_i s_i K_i$$

for some $s \in K$, whenever the left-hand side set is nonempty.

Proof. From the definition of the monomorphism φ_i it follows that $K = \bigcup_s sK'$ where $K' = \varphi_i(K_i)$ and s runs over a full system of representatives of K modulo K'. Moreover, for all $s, t \in K$ we have

$$sK' = tK' \;\Leftrightarrow\; s_j = t_j \text{ for all } j \ne i. \tag{11}$$

Besides,

$$a + rK = \bigcup_s (a + rsK') \tag{12}$$

for all $a, r \in R$. Suppose that the set $(a + rsK') \cap R_i$ is nonempty for some a, r and s. Then $a_j + r_j s_j = 0$ for all $j \neq i$. So if r is as in the lemma hypothesis, then the elements s_j for $j \neq i$, and hence by (11) the coset sK', are uniquely determined by a and r. Thus, in this case from (12) it follows that

$$(a + rK) \cap R_i = (a + rsK') \cap R_i = a_i + r_i s_i K_i.$$

Since the set $(a + rK) \cap R_i$ is nonempty iff the set $(a + rsK') \cap R_i$ is nonempty, we are done.■

Let us continue the proof of Lemma 3.1. First we observe that since $X + (v - v_i) = Y$, after translating by $v - v_i$ the equality of Lemma 3.2 with $a = v_i - v$ and $r = v - v_i$ we obtain that

$$rK \cap Y = \{v - v_i\}.$$

Denote by S the basis relation of the scheme $\mathcal{C}$ corresponding to r. Since the sets $rK = S_{out}(u)$ and Y are Δ_u-invariant, we conclude that so is the set $\{v - v_i\}$. Applying again Lemma 3.2 for $a = v - v_i$ and for r such that the set $(v - v_i + rK) \cap X$ is nonempty and $r_j \in R_j^\times$ for all $j \neq i$, we have

$$(v - v_i + rK) \cap X = r_i s_i K_i$$

for some $s \in K$. Since the sets $v - v_i + rK = S_{out}(v - v_i)$ and X are Δ_u-invariant, we conclude that so is the set $r_i s_i K_i$. Besides, all the sets $r_i s_i K_i$ cover X when r runs over all elements of R such that the set $(v - v_i + rK) \cap X$ is nonempty and $r_j \in R_j^\times$ for all $j \neq i$ (for instance, one can take $r_j = -1$ for $j \neq i$ and arbitrary $r_i \in R_i$). Thus any orbit of the group K_i is Δ_u-invariant.■

Thus the first part of Theorem 1.2 is proved. The second part follows from the first one and Lemma 2.4 applied to the schemes $\mathcal{C}$ and $\mathcal{C}_i$ for all i.

3.2 Proof of Theorem 1.3. Without loss of generality we assume that R is not a field. Then the required statement is a straightforward consequence of the following lemma the idea of the proof of which is taken from [7, Subsection 5.3].

Lemma 3.3 *In the conditions of Theorem 1.3 suppose that R is not a field and $K + I = K$ for some nonzero ideal I of R. Then $|R/\operatorname{rad}(R)| = 2$ and, moreover, $I \subset I_0$.*

Proof. For each $k \in 1 + I$ let us define a permutation f_k of R by

$$x^{f_k} = \begin{cases} kx, & \text{if } x \in \mathcal{U}; \\ x, & \text{if } x \notin \mathcal{U}. \end{cases} \tag{13}$$

We show that $f_k \in \mathrm{Aut}(\mathcal{C})$ where $\mathcal{C} = \mathrm{Cyc}(K, R)$. It suffices to verify that if $x - y \in rK$, then $x^{f_k} - y^{f_k} \in rK$ for all $x, y, r \in R$. This is obvious for $x, y \notin \mathcal{U}$, and follows from the inclusion $1 + I \leq K$ for $x, y \in \mathcal{U}$. If $x \in \mathcal{U}$ and $y \notin \mathcal{U}$, then

$$x^{f_k} - y^{f_k} = kx - y = k(x - y) + (k - 1)y \in rK + I = rK + rI = r(K + I) = rK$$

and we are done. The other case is treated similarly.

From the normality of $\mathcal{C}$ it follows that $x^{f_k} = ax^\sigma + b$ for some $a \in R^\times$, $b \in R$, $\sigma \in \mathrm{Aut}(R)$, and all $x \in R$. Since $0^{f_k} = 0$ and $1^{f_k} = k$, we conclude that $b = 0$ and $a = k$. Thus, $x^{f_k} = kx^\sigma$, $x \in R$. Due to the choice of k this implies that σ leaves fixed each element of $\mathcal{U}$ (and hence each element of $\mathrm{rad}(R)$) and each set $x + \mathrm{rad}(R)$. Since $\mathcal{T}^\sigma = \mathcal{T}$ and $|\mathcal{T} \cap (x + \mathrm{rad}(R))| = 1$ for $x \in R^\times$, it follows that σ leaves fixed each element of $\mathcal{T}$. Thus, $\sigma = \mathrm{id}_R$ and hence $x^{f_k} = kx$ for all $x \in R$. After comparing the latter equality with (13) we have

$$(k-1)x = 0, \qquad k \in 1 + I,\ x \in R \setminus \mathcal{U}. \tag{14}$$

Since $\mathrm{rad}(R) \subset R \setminus \mathcal{U}$, we conclude that $k - 1 \in I_0$ for all k and hence $I \subset I_0$. To complete the proof suppose that $|R/\mathrm{rad}(R)| > 2$. Then $R^\times \setminus \mathcal{U} \neq \emptyset$ and from (14) it follows that $Ix = 0$ for some $x \in R^\times$. So $I = 0$, which contradicts the choice of I.■

4 Multiplication S-ring of a cyclotomic scheme

Let $\mathcal{C} = \mathrm{Cyc}(K, R)$ be a cyclotomic scheme over a commutative ring R. Then from (6) it follows that $\Gamma(R^\times) \leq \mathrm{Iso}(\mathcal{C}_u)$ where $\mathcal{C}_u$ is the u-extension of $\mathcal{C}$ with $u = 0$. Since $\Delta(R^\times)$ is a relation of $\mathcal{C}_u$ and the set $R^\times$ is $\Gamma(R^\times)$-invariant, this implies that $R^\times_{right} = \Gamma(R^\times)^{R^\times}$ is a subgroup of $\mathrm{Iso}((\mathcal{C}_u)_{R^\times})$. So in accordance with Section 7 one can consider the scheme

$$\mathcal{C}' = ((\mathcal{C}_u)_{R^\times})^{R^\times_{right}}.$$

Obviously, $R^\times_{right} \leq \mathrm{Aut}(\mathcal{C}')$. Thus, $\mathcal{C}'$ is a Cayley scheme over the group $R^\times$. Denote by $\mathcal{A} = \mathcal{A}(K, R)$ the S-ring over $R^\times$ corresponding to the scheme $\mathcal{C}'$.

Definition 3 *The S-ring $\mathcal{A}$ is called the multiplication S-ring of the scheme $\mathcal{C}$.*

The multiplication S-ring of a cyclotomic scheme over a field was introduced and studied in [7].

Theorem 4.1 *The set $\mathcal{S}^*(\mathcal{A})$ contains both the sets rK for all $r \in R^\times$ and the sets $(1 + rK) \cap R^\times$ for all $r \in R$.*

Proof. Let $r \in R^\times$ and $C = rK$. Since each coset $C' \in R^\times/K$ is the neighborhood of u in the basis relation of $\mathcal{C}$ corresponding to C' , the set $\Delta(C')$ is a relation of the scheme $\mathcal{C}_u$. Therefore, so is the relation T defined by formula (25) with $G = R^\times$. Thus $C \in \mathcal{S}^*(\mathcal{A})$ because the relation T is $R^\times_{right}$-invariant and $T_{out}(1) = C$. To prove the second statement take $r \in R$ and set $X = (1 + rK) \cap R^\times$. It is easily seen that the smallest relation S of $\mathcal{C}_u$ containing $\{1\} \times X$ is a subset of $K \times R^\times$. Since all relations of $\mathcal{C}_u$ are $\Gamma(K)$-invariant, we see that $S_{out}(1) = X$. Besides, by the definition of the scheme $\mathcal{C}'$ the smallest relation S' of it containing S, is the union of all relations $Sr' = \{(sr', tr') :\ (s, t) \in S\}$ with $r' \in R^\times$. Since $S'_{out}(1) = S_{out}(1) = X$, it follows that $X \in \mathcal{S}^*(\mathcal{A})$ and we are done.■

The following theorem establishes some connection between the automorphism groups of the scheme $\mathcal{C}$ and the S-ring $\mathcal{A}$.

Theorem 4.2 *In the above notation let v be the identity of the ring R. Then*

(1) *the mapping* $f \mapsto f^{R^\times}$ *induces a homomorphism from* $\mathrm{Aut}(\mathcal{C}_{u,v})$ *to* $\mathrm{Aut}(\mathcal{A})$,

(2) *if* R *is a field, then the mapping from statement (1) is an isomorphism.*

Proof. The set $R^\times$ being the neighborhood of u in a relation of $\mathcal{C}$, is $\mathrm{Aut}(\mathcal{C}_u)$-invariant. So the mapping $f \mapsto f^{R^\times}$ induces a homomorphism from $\mathrm{Aut}(\mathcal{C}_u)$ to $\mathrm{Aut}(\mathcal{C}_u)^{R^\times}$. Besides,

$$\mathrm{Aut}(\mathcal{C}_u)^{R^\times} \le \mathrm{Aut}((\mathcal{C}_u)_{R^\times}) \le \mathrm{Aut}(\mathcal{C}').$$

Since $\mathrm{Aut}(\mathcal{C}')_v = \mathrm{Aut}(\mathcal{A})$ by the definition of the latter group, statement (1) follows. To prove statement (2) we note that the restriction homomorphism from $\mathrm{Aut}(\mathcal{C}_u)$ to $\mathrm{Aut}((\mathcal{C}_u)_{R^\times})$ is an isomorphism inducing the isomorphism from $\mathrm{Aut}(\mathcal{C}_{u,v})$ to $\mathrm{Aut}((\mathcal{C}_u)_{R^\times})_v$. On the other hand, by (23) with $\mathcal{C} = (\mathcal{C}_u)_{R^\times}$ and $\Gamma = R^\times_{right}$ we have $\mathrm{Aut}(\mathcal{C}') = R^\times_{right}\mathrm{Aut}((\mathcal{C}_u)_{R^\times})$. So $\mathrm{Aut}(\mathcal{A}) = \mathrm{Aut}(\mathcal{C}')_v = \mathrm{Aut}((\mathcal{C}_u)_{R^\times})_v$ and we are done.■

In the general case the relationship between the groups $\mathrm{Aut}(\mathcal{C}_{u,v})$ and $\mathrm{Aut}(\mathcal{A})$ is unclear. However, we have the following statement to be used in Section 6.

Theorem 4.3 *Let* R *be a local commutative ring,* $\mathcal{C} = \mathrm{Cyc}(K, R)$ *and* $\mathcal{A} = \mathcal{A}(K, R)$. *Then the scheme* $\mathcal{C}_{u,v}$ *is trivial whenever the S-ring* $\mathcal{A}$ *is trivial. In particular, in this case* $\mathrm{Aut}(\mathcal{C}) = \Gamma(K, R)$.

Proof. Suppose that the S-ring $\mathcal{A}$ is trivial. This means that $\mathcal{C}'$ is the scheme of 2-orbits of the group $R^\times_{right}$ and consequently the scheme $(\mathcal{C}')_v$ is trivial. So both the scheme $((\mathcal{C}_u)_{R^\times})_v$ and its extension $(\mathcal{C}_{u,v})_{R^\times}$ are trivial too. On the other hand, the permutation $s = \gamma_{-1,1}$ is an isomorphism of the scheme $\mathcal{C}$ that interchanges u and v. So $s \in \mathrm{Iso}(\mathcal{C}_{u,v})$. Thus, the scheme $(\mathcal{C}_{u^s,v^s})_{(R^\times)^s} = (\mathcal{C}_{v,u})_{1-R^\times}$ is trivial. It follows that the restriction of $\mathcal{C}_{u,v}$ to the set $R^\times \cup (1 - R^\times)$ is trivial. Due to the locality of the ring R we have $R = R^\times \cup (1 - R^\times)$. Thus the scheme $\mathcal{C}_{u,v}$ is trivial. The second part of the theorem follows from the first one and the proof of Lemma 2.4.■

5 Multiplication S-ring: pure case

In this section the multiplication S-ring of a cyclotomic scheme $\mathrm{Cyc}(K, R)$ is studied for a pure group $K \le \mathcal{T}\mathcal{U}_0$. First we rewrite the second half of the sets from Theorem 4.1 in the multiplicative form.

Lemma 5.1 *Let* R *be a finite local commutative ring and* $K = \mathcal{T}(1 + H) \le R^\times$ *with* $H \le I_0$. *Then given* $r = 1 + x \in \mathcal{U}$ *we have*

$$(1 + rK) \cap R^\times = \bigcup_{t \in \mathcal{T},\ t \ne 1} t(1 + z_{t,x} + \frac{t-1}{t}(H + x))$$

where $z_{t,x} = y_t r$ *with the element* $y_t \in \mathrm{rad}(R)$ *uniquely determined by the condition* $1 - t^{-1} + y_t \in \mathcal{T}$.

Proof. From (3) it follows

$$(1 + rK) \cap R^\times = \bigcup_{t \in \mathcal{T},\ t \ne 1} ((1 + rK) \cap t\mathcal{U}). \tag{15}$$

Let $t \in \mathcal{T}$, $1 + t \notin \mathrm{rad}(R)$. Then $1 + t = t'(1 + y_{t'})$ for some $t' \in \mathcal{T}$. So

$$(1 + rK) \cap t\mathcal{U} = 1 + (1 + x)t(1 + H) = 1 + t(1 + H + x) = (1 + t)(1 + \frac{t}{1 + t}(H + x)) =$$

$$t'(1 + y_{t'})(1 + \frac{t'(1 + y_{t'}) - 1}{t'(1 + y_{t'})}(H + x)) = t'(1 + y_{t'} + \frac{t'(1 + y_{t'}) - 1}{t'}(H + x)) =$$

$$t'(1 + y_{t'} + y_{t'}x + \frac{t' - 1}{t'}(H + x)) = t'(1 + z_{t',x} + \frac{t' - 1}{t'}(H + x))$$

(here $xH = y_{t'}H = \{0\}$ because $H \leq I_0$). To complete the proof, due to (15) it suffices to note that t' runs over the set $\mathcal{T} \setminus \{1\}$ when t runs over the set $\mathcal{T} \setminus (-1 + \mathrm{rad}(R))$.■

Theorem 5.2 *Let R be a finite local commutative ring, K a subgroup of $R^\times$ and $\mathcal{A}$ an S-ring over $R^\times$ such that $X(r) \in \mathcal{S}^*(\mathcal{A})$ for all $r \in R$ where $X(r) = (1 + rK) \cap R^\times$. Suppose that $K \leq \mathcal{T}\mathcal{U}_0$ and the group K is pure. Then*

(1) *$\mathcal{T}$,$\mathcal{U} \in \mathcal{H}(\mathcal{A})$,*

(2) *the S-ring $\mathcal{A}$ is trivial whenever so is the S-ring $\mathcal{A}_\mathcal{T}$ or the S-ring $\mathcal{A}_\mathcal{U}$.*

Before proving Theorem 5.2 we deduce from it an easy corollary to be used in the next section.

Theorem 5.3 *Let R be a finite local commutative ring and $\mathcal{A} = \mathcal{A}(K, R)$ where the group K is as in Theorem 5.2. Then*

(1) *$\mathcal{T}$,$\mathcal{U} \in \mathcal{H}(\mathcal{A})$*

(2) *if $H \in \{\mathcal{T}, \mathcal{U}\}$, then the S-ring generated by $\mathcal{A}$ and the cosets of $R^\times$ by H is trivial.*

Proof. Statement (1) immediately follows from statement (1) of Theorem 5.2. because the S-ring $\mathcal{A}$ satisfies the hypothesis of this theorem (see Theorem 4.1). To prove statement (2) denote by $\mathcal{A}'$ the S-ring generated by $\mathcal{A}$ and the cosets of $R^\times$ by H. Since $\mathcal{A}' \geq \mathcal{A}$, the S-ring $\mathcal{A}'$ satisfies the hypothesis of Theorem 5.2. So by statement (2) of that theorem it suffices to verify that the S-ring $\mathcal{A}'_{H'}$ is trivial where $H' = \mathcal{U}$ if $H = \mathcal{T}$, and $H' = \mathcal{T}$ if $H = \mathcal{U}$. However, this follows from the fact that $|H' \cap C| = 1$ for any coset $C \subset R^\times$ by the group H.■

Proof of Theorem 5.2. Since $\mathcal{U}$ is the complement of the set $\bigcup_{r \in R^\times} X(r)$ in $R^\times$, the second part of statement (1) follows. To prove the rest of the theorem we need the following lemma.

Lemma 5.4 *In the condition of the theorem we have:*

(1) *if $[tu_1] = [tu_2]$ for some generator t of $\mathcal{T}$ where $u_1, u_2 \in \mathcal{U}$, then $u_1 = u_2$,*

(2) *if $[t_1u] = [t_2u]$ for all $u \in \mathcal{U}$ where $t_1, t_2 \in \mathcal{T}$, then $t_1 = t_2$.*

Proof. Without loss of generality we assume that $\mathcal{T} \leq K$. First, we prove statement (1). Any set $X \subset R^\times$ can uniquely be represented in the form $X = \bigcup_{t\in\mathcal{T}} tX_t$ where $X_t \subset \mathcal{U}$ (see (3)). It follows that for any $\sigma \in \mathrm{Aut}(\mathcal{T})$ we have

$$X_t = (X^{\widehat{\sigma}})_{t^\sigma}, \quad t \in \mathcal{T}, \tag{16}$$

where $\widehat{\sigma}$ is an automorphism of $R^\times$ such that $\widehat{\sigma}^{\mathcal{T}} = \sigma$ and $\widehat{\sigma}^{\mathcal{U}} = \mathrm{id}_{\mathcal{U}}$. Since the group $\mathcal{T}$ is cyclic and its order is coprime to $|\mathcal{U}|$, the Chinese Remainder Theorem implies that the automorphism $\widehat{\sigma}$ is induced by raising to a power coprime to $|R^\times|$.

Now let $X = [tu]$ where t is a generator of $\mathcal{T}$ and $u \in \mathcal{U}$. Then obviously $u \in X_t$ and it suffices to verify that

$$X_t = \{u\}. \tag{17}$$

To do this we note that by the Schur theorem on multipliers $X^{\widehat{\sigma}} = [t^\sigma u]$ for all $\sigma \in \mathrm{Aut}(\mathcal{T})$. So $X^{\widehat{\sigma}} \subset X(r_\sigma)$ for some $r_\sigma = 1 + x_\sigma$ with $x_\sigma \in \mathrm{rad}(R)$ (we made used of the fact that the latter set belongs to $\mathcal{S}^*(\mathcal{A})$ and the union of all such sets equals $R^\times \setminus \mathcal{U}$). Since $K \cap \mathcal{U} = 1 + H$ where $H \leq I_0$, this implies by Lemma 5.1 that

$$(X^{\widehat{\sigma}})_{t^\sigma} \subset 1 + z_{t^\sigma, x_\sigma} + \frac{t^\sigma - 1}{t^\sigma}(H + x_\sigma).$$

However by (16) the element u belongs to the left-hand side and so the right-hand side being a coset by the group $\frac{t^\sigma-1}{t^\sigma}H$, equals $u + \frac{t^\sigma-1}{t^\sigma}H$. Thus,

$$X_t \subset \bigcap_{\sigma\in\mathrm{Aut}(\mathcal{T})} (u + \frac{t^\sigma - 1}{t^\sigma}H) = u + H_0$$

where H_0 is the intersection of all groups $\frac{t^\sigma-1}{t^\sigma}H$. To complete the proof of (17) we will show that $H_0 = \{0\}$. Suppose on the contrary that there exists a nonzero $x \in H_0$. Then $\frac{1}{1-t^\sigma}x \in H$ for all $\sigma \in \mathrm{Aut}(\mathcal{T})$. On the other hand, the following equality is true

$$\frac{d}{1 - t^d} = \sum_{i=0}^{d-1} \frac{1}{1 - r^i t},$$

where d is a proper divisor of $|\mathcal{T}|$ and r is a generator of the subgroup of $\mathcal{T}$ of order d. (It follows from the identity $\frac{f'(x)}{f(x)} = \sum_{i=0}^{d-1} \frac{1}{x-x_i}$ where $f(x) = \prod_{i=0}^{d-1}(x - x_i)$ with $x_i \in R$, if we take $f(x) = x^d - 1 = \prod_{i=0}^{d-1}(x - r^i)$ and put $x = t^{-1}$.) Since d is coprime to the characteristic of R and $r^i t$ is a generator of $\mathcal{T}$ for all i, the subgroup of R^+ generated by the set $\{\frac{1}{1-t^\sigma},\ \sigma \in \mathrm{Aut}(\mathcal{T})\}$ contains the set $M = \{\frac{1}{1-t'} :\ t' \in \mathcal{T} \setminus \{1\}\}$. Thus, $Mx \subset H$. Since the image of M in the residue field $\mathbb{F}$ of R equals $\mathbb{F}^\times \setminus \{1\}$ and $x \in I_0$, we have $Mx = Rx$. So $1 + I \subset 1 + H \subset K$ where $I = Rx$, which contradicts the purity of K. This completes the proof of statement (1).

To prove statement (2) suppose that $[t_1 u] = [t_2 u]$ for all $u \in \mathcal{U}$ where $t_1, t_2 \in \mathcal{T}$. By the second part of statement (1) without loss of generality we can assume that $t_1 \neq 1$ and $t_2 \neq 1$. It suffices to verify that if $t_1 \neq t_2$, then there exists $r \in \mathcal{U}$ such that

$$t_1^{-1}(1 + rK) \cap \mathcal{U} \neq t_2^{-1}(1 + rK) \cap \mathcal{U}. \tag{18}$$

Indeed, in this case there exists an element u belonging to the left-hand side but not belonging to the right-hand side (or vice versa). Then $t_1 u \in X(r)$ and $t_2 u \notin X(r)$. Since

$X(r) \in \mathcal{S}^*(\mathcal{A})$, this implies that $[t_1u] \neq [t_2u]$, which contradicts the supposition. To prove the required statement let $r = 1 + x \in \mathcal{U}$ be such that (18) becomes equality. Then from Lemma 5.1 it follows that

$$1 + z_{t_1,x} + \frac{t_1 - 1}{t_1}(H + x) = 1 + z_{t_2,x} + \frac{t_2 - 1}{t_2}(H + x) \tag{19}$$

where H is as above. Since the left-hand and right-hand sides are cosets by the groups $\frac{t_1-1}{t_1}H$ and $\frac{t_2-1}{t_2}H$ respectively, these groups are equal. Moreover, from (19) it follows that

$$sx \in y + H'$$

where $s = y_{t_1} - y_{t_2} + \frac{t_1-1}{t_1} - \frac{t_2-1}{t_2}$, $y = y_{t_2} - y_{t_1}$ (see Lemma 5.1) and $H' = \frac{t_1-1}{t_1}H = \frac{t_2-1}{t_2}H$. We observe that $y \in \mathrm{rad}(R)$, and $s \in R^\times$ because $t_1 \neq t_2$. It follows that x belongs to the coset

$$C = s^{-1}y + s^{-1}H' \subset I_0.$$

On the other hand, due to the purity of K we have $H \neq I_0$ and hence $s^{-1}H' \neq I_0$. Thus, $C \subsetneqq I_0$ and inequality (18) is satisfied for any $r = 1 + x$ with $x \in I_0 \setminus C$.■

To prove the first part of statement (1) take a generator t of the group $\mathcal{T}$. It suffices to verify that the set $X = [t]$ is contained in $\mathcal{T}$. To do this we observe that from statement (1) of Lemma 5.4 it follows that $t^p \in X^{[p]}$ where p is the characteristic of the residue field of R and $X^{[p]}$ is as in the Schur theorem on multipliers. So $t \in X' = (X^{[p]})^{\widehat{\sigma}}$ where σ is the automorphism of $\mathcal{T}$ inverse to raising to the pth degree and $\widehat{\sigma}$ is the automorphism of $R^\times$ defined above. Then by the Schur theorem on multipliers $X' \in \mathcal{S}^*(\mathcal{A})$ and hence $X \subset X'$. To complete the proof of statement (1) it suffices to observe that $|X'| \leq |X|$ with the equality attained iff $X \subset \mathcal{T}$.

To prove statement (2) suppose that the S-ring $\mathcal{A}_\mathcal{T}$ is trivial. Let $u_1, u_2 \in \mathcal{U}$, $u_1 \neq u_2$. Then from statement (1) of Lemma 5.4 it follows that $[tu_1] \neq [tu_2]$ for some $t \in \mathcal{T}$. Since $[t] = \{t\}$, we have $[tu_i] = [t][u_i]$ for $i = 1, 2$, whence it follows that $[u_1] \neq [u_2]$. Thus the S-ring $\mathcal{A}_\mathcal{U}$ is trivial and consequently so is the S-ring $\mathcal{A}$. The second part of the statement is proved in a similar way by using statement (2) of Lemma 5.4.■

6 Strongly pure groups and proof of Theorem 1.4

6.1 Reduction statement. For a cyclotomic scheme $\mathcal{C}$ over a ring R we set

$$\mathrm{Aut}_\mathcal{C}(R) = \mathrm{Aut}(\mathcal{C}) \cap \mathrm{Aut}(R).$$

If I is an ideal of R, we write $\mathrm{Aut}_\mathcal{C}(R/I)$ instead of $\mathrm{Aut}_{\mathcal{C}_{R/E(I)}}(R/I)$.

Theorem 6.1 *Let R be a finite local commutative ring and $\mathcal{C} = \mathrm{Cyc}(K, R)$ where $K \leq R^\times$ is a pure group. Then the natural mapping $\mathrm{Aut}_\mathcal{C}(R) \to \mathrm{Aut}_\mathcal{C}(R/I_0)$ is a monomorphism. Moreover, $\mathrm{Aut}(\mathcal{C}) \leq \mathrm{A\Gamma L}_1(R)$ whenever $\mathrm{Aut}(\mathcal{C})^{R/E_0} \leq \mathrm{A\Gamma L}_1(R/I_0)$ where $E_0 = E_{I_0}$.*

Proof. We observe that the kernel of the homomorphism $f \mapsto f^{R/E_0}$ from $\mathrm{Aut}(\mathcal{C})$ to $\mathrm{Aut}(\mathcal{C})^{R/E_0}$ coincides with the group $\mathrm{Aut}(\mathcal{C})_{E_0}$. Moreover,

$$\mathrm{Aut}(\mathcal{C})_{E_0} \leq \mathrm{AGL}_1(R). \tag{20}$$

Indeed, $\mathcal{C}_{E_0} \geq \mathrm{Cyc}(U_0, R)$ by Theorem 2.5. So $\mathrm{Aut}(\mathcal{C})_{E_0} = \mathrm{Aut}(\mathcal{C}_{E_0}) \leq \mathrm{Aut}(\mathrm{Cyc}(U_0, R))$. By Theorem 4.3 it suffices to verify that the S-ring $\mathcal{A}(U_0, R)$ is trivial. However, the latter immediately follows from Theorem 5.3.

Let $f \in \mathrm{Aut}_{\mathcal{C}}(R)$ be such that f^{R/E_0} is identical. Then $f \in \mathrm{Aut}(\mathcal{C}_{E_0})$ and hence $f \in \mathrm{AGL}_1(R)$ by (20). Since obviously f leaves fixed the points 0 and 1, this implies that $f = \mathrm{id}_R$. Thus the first statement of the theorem is proved.

To prove the second statement suppose that $\mathrm{Aut}(\mathcal{C})^{R/E_0} \leq \mathrm{A\Gamma L}_1(R/I_0)$. Then by Lemma 2.1 with $K = R^\times$ it suffices to verify due to the locality of R that the group $\Gamma = \Gamma(R^\times, R)$ is normalized by $\mathrm{Aut}(\mathcal{C})$. By (20) all we need to prove is

$$f^{-1}\Gamma f \subset \Gamma\,\mathrm{Aut}(\mathcal{C}_{E_0}), \quad f \in \mathrm{Aut}(\mathcal{C}).$$

Take $\gamma \in \Gamma$ and $f \in \mathrm{Aut}(\mathcal{C})$. Then

$$\overline{f^{-1}\gamma f} = \overline{f}^{-1}\overline{\gamma}\overline{f} \in \overline{f}^{-1}\overline{\Gamma f} = \overline{\Gamma} \tag{21}$$

where the bar means factorization modulo E_0 (we made used of the fact that due to the assumption $\overline{f} \in \overline{\mathrm{Aut}(\mathcal{C})} \leq \mathrm{A\Gamma L}_1(R/I_0)$). On the other hand, $f^{-1}\gamma f = \gamma(\gamma^{-1}f^{-1}\gamma)f = \gamma f_1$ where $f_1 = (\gamma^{-1}f^{-1}\gamma)f$. Since $\Gamma \leq \mathrm{Iso}(\mathcal{C})$, we have $f_1 \in \mathrm{Aut}(\mathcal{C})$. So from (21) it follows that

$$\overline{f_1} \in \overline{\Gamma} \cap \overline{\mathrm{Aut}(\mathcal{C})} = \Gamma(\overline{K}, \overline{R})$$

where $\overline{K} = \pi_0(K)$ and $\overline{R} = R/I_0$. Due to the surjectivity of the natural homomorphism $\Gamma(K, R) \to \Gamma(\overline{K}, \overline{R})$, this implies that there exists $\gamma_1 \in \Gamma(K, R)$ such that $\overline{\gamma_1} = \overline{f_1}$. Thus, $\gamma_1^{-1}f_1 \in \mathrm{Aut}(\mathcal{C}_{E_0})$ and consequently

$$f^{-1}\gamma f = (\gamma\gamma_1)(\gamma_1^{-1}f_1) \in \Gamma\,\mathrm{Aut}(\mathcal{C}_{E_0}).\blacksquare$$

6.2 Strongly pure groups and normality. We deduce Theorem 1.4 from a more general result by using the notion of strong purity recursively defined as follows. A group $K \leq R^\times$ is called *strongly pure* if it is pure and the group $\pi_0(K)$ is strongly pure unless R is a field. Obviously, any strongly pure group is pure. The converse statement is not true in the general case: a counterexample is given by $R = \mathbb{F}[X]/(X^n)$ where $\mathbb{F}$ is a finite field, $n \geq 3$, and $K = 1 + \mathbb{F}x^{n-2}$ with $x = X \mod X^n$. However from the definition it immediately follows that it is true whenever $\mathrm{rad}(R)^2 = \{0\}$.

Theorem 6.2 *Let R be a finite local commutative ring other than a field. Then $\mathcal{C} = \mathrm{Cyc}(K, R)$ is a normal scheme whenever K is a strongly pure group. Moreover, in this case the natural mapping $\mathrm{Aut}_{\mathcal{C}}(R) \to \mathrm{Aut}_{\mathcal{C}}(\mathbb{F})$ is a monomorphism where $\mathbb{F}$ is the residue field of R.*

Proof. With the help of Theorem 6.1 applying inductively, the proof is reduced to the case $\mathrm{rad}(R)^2 = \{0\}$. Then the group K is pure. Thus the statement on monomorphism immediately follows from the first part of that theorem. To complete the proof, assume (without loss of generality) that $K \geq \mathcal{T}$. Then due to the second part of the same theorem it suffices to verify that

$$\mathrm{Aut}(\mathcal{C})^{\mathbb{F}} \leq \mathrm{A\Gamma L}_1(\mathbb{F}). \tag{22}$$

To do this we need the following lemma.

Lemma 6.3 *The groups* $\mathrm{Aut}(\mathcal{C}_u)^{R^\times}$ *and* $\mathrm{Aut}(\mathcal{C}_v)^{1-R^\times}$ *normalize the groups* $\Gamma(\mathcal{T})^{R^\times}$ *and* $(s\Gamma(\mathcal{T})s)^{1-R^\times}$ *respectively where* $u=0$, $v=1$ *and* $s=\gamma_{-1,1}$.

Proof. From statement (1) of Theorem 5.3 it follows that $\mathcal{T}\in\mathcal{H}(\mathcal{A})$ where $\mathcal{A}$ is the multiplication S-ring of the scheme $\mathcal{C}$. So Theorem 7.2 (with $H=\mathcal{T}$) implies that $\mathrm{Aut}(\mathcal{A})$ normalizes the group $\langle \mathrm{Aut}(\mathcal{A}'), \Gamma(\mathcal{T})^{R^\times}\rangle$. However, in our case the group $\mathrm{Aut}(\mathcal{A}')$ is trivial by statement (2) of Theorem 5.3. Therefore, $\mathrm{Aut}(\mathcal{A})$ normalizes $\Gamma(\mathcal{T})^{R^\times}$. On the other hand, from the definition of the S-ring $\mathcal{A}$ it follows that $\mathrm{Aut}(\mathcal{C}_u)^{R^\times}\le \Gamma(R^\times)^{R^\times}\,\mathrm{Aut}(\mathcal{A})$. Thus, $\mathrm{Aut}(\mathcal{C}_u)^{R^\times}$ normalizes the group $\Gamma(\mathcal{T})^{R^\times}$. To complete the proof we observe that obviously s is an isomorphism of $\mathcal{C}$ that interchanges u and v. Thus the group $\mathrm{Aut}(\mathcal{C}_v)^{1-R^\times}$ normalizes the group $(s\Gamma(\mathcal{T})s)^{1-R^\times}$.■

To prove (22) it suffices to show that if $\gamma\in\mathrm{Aut}(\mathcal{C}_{u,v})$, then $\gamma^{\mathbb{F}}\in\mathrm{Aut}(\mathbb{F})$. However, from Lemma 6.3 it follows that the permutation $\gamma^{X_0}=(\gamma^{R^\times})^{X_0}$ normalizes the group $\Gamma(\mathbb{F}^\times)^{X_0}$ whereas the permutation $\gamma^{X_1}=(\gamma^{1-R^\times})^{X_1}$ normalizes the group $(s^{\mathbb{F}}\Gamma(\mathbb{F}^\times)s^{\mathbb{F}})^{X_1}$ where $X_i=\mathbb{F}\setminus\{i\}$, $i\in\{0_{\mathbb{F}},1_{\mathbb{F}}\}$. Thus, $\gamma^{\mathbb{F}}$ normalizes both the groups $\Gamma(\mathbb{F}^\times)$ and $s^{\mathbb{F}}\Gamma(\mathbb{F}^\times)s^{\mathbb{F}}$ and we are done by Corollary 2.2.■

Since a pure group $K\le\mathcal{TU}_0$ is obviously strongly pure, from Theorem 6.2 we obtain the following statement.

Theorem 6.4 *Let* R *be a finite local commutative ring other than a field and* K *a pure subgroup of* $R^\times$. *Then the scheme* $\mathrm{Cyc}(K,R)$ *is normal whenever* $K\le\mathcal{TU}_0$.■

We complete the subsection by giving a sufficient condition for the automorphism group of a cyclotomic scheme to be a subgroup of $\mathrm{AGL}_1(R)$.

Theorem 6.5 *Let* $\mathcal{C}=\mathrm{Cyc}(K,R)$ *be a cyclotomic scheme over a finite local commutative ring* R *other than a field. Then* $\mathrm{Aut}(\mathcal{C})\le\mathrm{AGL}_1(R)$ *whenever one of the following conditions is satisfied:*

(1) $K\le\mathcal{T}$,

(2) K *is a strongly pure subgroup of* $\mathcal{U}$,

(3) *the group* K *is strongly pure and the residue field of* R *is prime.*

Proof. To prove statement (1) we observe that from Theorem 4.1 it follows that the S-ring $\mathcal{A}(K,R)$ contains all elements of the set $R^\times/K$. So by statement (2) of Theorem 5.3 this S-ring is trivial and we are done by Theorem 4.3. To prove statements (2) and (3) we observe that from the first part of Theorem 6.2 it follows that $\mathrm{Aut}(\mathcal{C})\le\mathrm{A\Gamma L}_1(R)$. So by the second part of this theorem it suffices to prove that the group $\mathrm{Aut}_{\mathcal{C}}(\mathbb{F})$ is trivial where $\mathbb{F}$ is the residue field of R. However, for statement (2) this is clear because $\mathcal{C}_{\mathbb{F}}=\mathrm{Cyc}(\{1\},\mathbb{F})$ (see (7)) whereas for statement (3) because $\mathrm{Aut}(\mathbb{F})=\{1\}$.■

6.3 Proof of Theorem 1.4. By Theorem 6.2 the required statement is the consequence of the following theorem.

Theorem 6.6 *For a Galois ring of odd characteristic any pure group is strongly pure.*

Proof. Let $R = \mathrm{GR}(p^n, r)$ where p is odd. We can assume that $n > 1$. Then the group $\mathcal{U}$ is isomorphic to the direct product of r copies of a cyclic group of order p^{n-1} (see [5]). In particular, $\mathrm{rk}(\mathcal{U}) = r$ and the maximal elementary abelian subgroup of $\mathcal{U}$ equals $\mathcal{U}_0$. Since the rank of an abelian group does not increase by factorization, the theorem follows by induction from the lemma below.

Lemma 6.7 *Under the above assumptions a group $K \le R^\times$ is pure iff* $\mathrm{rk}(U) < r$ *where* $U = K \cap \mathcal{U}$.

Proof. Suppose that the group K is not pure. Then $\mathcal{U}_0 \le U$. On the other hand, since $I_0 = p^{n-1}R$, the group $\mathcal{U}_0$ is an elementary abelian of order p^r. Thus, $\mathrm{rk}(U) \ge \mathrm{rk}(\mathcal{U}_0) = r$. Conversely, let $\mathrm{rk}(U) = r$. Then the maximal elementary abelian subgroup of U is of order p^r. So it coincides with the maximal elementary abelian subgroup of $\mathcal{U}$. Since the latter subgroup equals $\mathcal{U}_0$, we are done.∎

7 Appendix

7.1 Schemes. Let V be a finite set and $\mathcal{R}$ a partition of V^2 closed with respect to transposition.[3] Denote by $\mathcal{R}^*$ the set of all unions of the elements of $\mathcal{R}$. A pair $\mathcal{C} = (V, \mathcal{R})$ is called a *coherent configuration* or a *scheme* on V if the diagonal $\Delta(V)$ of V^2 belongs to $\mathcal{R}^*$ and given $R, S, T \in \mathcal{R}$, the number $|\{v \in V : (u, v) \in R,\ (v, w) \in S\}|$ does not depend on the choice of $(u, w) \in T$. The elements of V, $\mathcal{R} = \mathcal{R}(\mathcal{C})$ and $\mathcal{R}^* = \mathcal{R}^*(\mathcal{C})$ are called the *points*, the *basis relations* and the *relations* of $\mathcal{C}$, respectively. The number $\mathrm{rk}(\mathcal{C}) = |\mathcal{R}|$ is called the *rank* of $\mathcal{C}$. We observe that given $X, Y \subset V$ we have $X \times Y \in \mathcal{R}^*$ whenever $\Delta(X), \Delta(Y) \in \mathcal{R}^*$.

Two schemes are called *isomorphic* if there exists a bijection between their point sets preserving the basis relations. Any such bijection is called an *isomorphism* of these schemes. The set of all isomorphisms of a scheme $\mathcal{C}$ is denoted by $\mathrm{Iso}(\mathcal{C})$. This group contains a normal subgroup

$$\mathrm{Aut}(\mathcal{C}) = \{f \in \mathrm{Sym}(V) :\ R^f = R,\ R \in \mathcal{R}\}$$

called the *automorphism group* of $\mathcal{C}$. For a group $\Gamma \le \mathrm{Iso}(\mathcal{C})$ we denote by $\mathcal{C}^\Gamma$ the scheme on the same point set the relations of which are exactly the elements of $\mathcal{R}^*$ invariant with respect to Γ. In particular, if the scheme $\mathcal{C}$ is *trivial*, i.e. $\mathcal{R}^* = 2^{V^2}$, then $\mathrm{Iso}(\mathcal{C}) = \mathrm{Sym}(V)$ and $\mathcal{C}^\Gamma$ equals the *scheme of 2-orbits* of the group Γ. In the general case, it can be proved that if Γ acts regularly on the set $\{X \subset V :\ \Delta(X) \in \mathcal{R}\}$, then

$$\mathrm{Aut}(\mathcal{C}^\Gamma) = \Gamma\, \mathrm{Aut}(\mathcal{C}) \tag{23}$$

(see [7, Theorem 2.2]).

Given a set $U \subset V$ denote by $\mathcal{R}_U$ the set of all nonempty relations $R_U = R \cap U^2$, $R \in \mathcal{R}$ (treated as relations on U). If $\Delta(U) \in \mathcal{R}^*$, then $\mathcal{C}_U = (U, \mathcal{R}_U)$ is a scheme on U. Clearly,

$$\mathrm{Aut}(\mathcal{C})^U \le \mathrm{Aut}(\mathcal{C}_U).$$

[3]The elements of $\mathcal{R}$ are assumed to be nonempty.

Given an equivalence relation E on V denote by $\mathcal{R}_{V/E}$ the set of all relations

$$R_{V/E} = \{(X, Y) \in (V/E)^2 : \ R \cap (X \times Y) \neq \emptyset\}$$

where $R \in \mathcal{R}$. If $E \in \mathcal{R}^*$, then $\mathcal{C}_{V/E} = (V/E, \mathcal{R}_{V/E})$ is a scheme on V/E. The set of all such E is denoted by $\mathcal{E} = \mathcal{E}(\mathcal{C})$. Clearly,

$$\mathrm{Aut}(\mathcal{C})^{V/E} \leq \mathrm{Aut}(\mathcal{C}_{V/E}).$$

The set of all schemes on V is partially ordered by inclusion: namely, $\mathcal{C} \leq \mathcal{C}'$ iff $\mathcal{R}^* \subset (\mathcal{R}')^*$. The largest scheme is the trivial scheme on V whereas the smallest one is the scheme of 2-orbits of the group $\mathrm{Sym}(V)$. For sets $\mathcal{R}_1, \ldots, \mathcal{R}_s$ of binary relations on V we denote by $[\mathcal{R}_1, \ldots, \mathcal{R}_s]$ the smallest scheme $\mathcal{C}$ on V such that $\mathcal{R}_i \subset \mathcal{R}^*$ for all i; we omit the braces if $\mathcal{R}_i = \{R_i\}$ and write $\mathcal{C}_i$ instead of $\mathcal{R}_i$ if the latter is the set of basis relations of $\mathcal{C}_i$. In particular, if $\mathcal{C}$ is a scheme on V and $v_1, \ldots, v_s \in V$, then we set $\mathcal{C}_{v_1,\ldots,v_s} = [\mathcal{C}, \Delta(\{v_1\}), \ldots, \Delta(\{v_s\})]$. One can see that

$$\mathrm{Aut}(\mathcal{C}_{v_1,\ldots,v_s}) = \mathrm{Aut}(\mathcal{C})_{v_1,\ldots,v_s}$$

where $\mathrm{Aut}(\mathcal{C})_{v_1,\ldots,v_s}$ is the pointwise stabilizer of the set $\{v_1, \ldots, v_s\}$ in the group $\mathrm{Aut}(\mathcal{C})$. We will also use the following property of the *v-extension* $\mathcal{C}_v$ of the scheme $\mathcal{C}$ where $v \in V$: if $X = R_{out}(v)$ is the neighborhood of v in a relation $R \in \mathcal{R}^*$, then $\Delta(X)$ is a relation of $\mathcal{C}_v$. Finally, if E is an equivalence relation on V, we set $\mathcal{C}_E = [\mathcal{C}, \{\Delta(X) : \ X \in V/E\}]$. It immediately follows that

$$\mathrm{Aut}(\mathcal{C}_E) \trianglelefteq \mathrm{Aut}(\mathcal{C}), \quad E \in \mathcal{E}(\mathcal{C}). \tag{24}$$

7.2 S-rings. Let G be a finite group. A subring $\mathcal{A}$ of the group ring $\mathbb{Z}[G]$ is called a *Schur ring* (*S-ring*, for short) over G if it has a (uniquely determined) $\mathbb{Z}$-base consisting of the elements $\sum_{x \in X} x$ where X runs over a family $\mathcal{S} = \mathcal{S}(\mathcal{A})$ of pairwise disjoint nonempty subsets of G such that

$$\{1\} \in \mathcal{S}, \quad \bigcup_{X \in \mathcal{S}} X = G \quad \text{and} \quad X \in \mathcal{S} \ \Rightarrow \ X^{-1} \in \mathcal{S}.$$

We call the elements of $\mathcal{S}$ *basic sets* of $\mathcal{A}$ and denote by $\mathcal{S}^* = \mathcal{S}^*(\mathcal{A})$ the set of all unions of them and by $\mathcal{H} = \mathcal{H}(\mathcal{A})$ the set of all *$\mathcal{A}$-subgroups* of G (i.e. those belonging to $\mathcal{S}^*$). The basic set of $\mathcal{A}$ that contains $x \in G$ is denoted by $[x]$. The number $\mathrm{rk}(\mathcal{A}) = \dim_{\mathbb{Z}}(\mathcal{A})$ is called the *rank* of $\mathcal{A}$. When $\mathrm{rk}(\mathcal{A}) = |G|$ (equivalently, $\mathcal{A} = \mathbb{Z}[G]$) we call the S-ring $\mathcal{A}$ *trivial*. Given $H \in \mathcal{H}$ denote by $\mathcal{A}_H$ the S-ring over H with $\mathcal{S}(\mathcal{A}_H) = \{X \in \mathcal{S} : \ X \subset H\}$.

The proof of the following theorem called the *Schur theorem on multipliers* can be found in [10]. Below given $X \subset G$ we set $X^{(m)} = \{x^m : \ x \in X\}$ for all $m \in \mathbb{Z}$, and $X^{[p]} = \{x^p : \ x \in X, \ |xH \cap X| \not\equiv 0 \pmod p\}$ for all prime p where $H = \{g \in G : \ g^p = 1\}$.

Theorem 7.1 *Let G be a finite abelian group and $\mathcal{A}$ an S-ring over G. Then for any $X \in \mathcal{S}(\mathcal{A})$ the following statements hold:*

(1) $X^{(m)} \in \mathcal{S}(\mathcal{A})$ *for any integer m coprime to $|G|$,*

(2) $X^{[p]} \in \mathcal{S}^*(\mathcal{A})$ *for any prime p dividing $|G|$.* ∎

For a finite group G denote by $\mathcal{R}(G)$ the set of all binary relations on G that are invariant with respect to G_{right}. Then the mapping

$$2^G \to \mathcal{R}(G), \quad X \mapsto R_G(X)$$

where $R_G(X) = \{(g, xg) : \ g \in G, x \in X\}$, is a bijection. A straightforward computation shows that if $H \lhd G$ and $C \in G/H$, then

$$R_G(C) = \bigcup_{C' \in G/H} C' \times CC'.^4 \tag{25}$$

In particular, $R_G(H)$ is an equivalence relation on G.

Let $\mathcal{A}$ be an S-ring over the group G. Then the pair $\mathcal{C} = (G, \mathcal{R})$ where $\mathcal{R} = R_G(\mathcal{S})$, is a scheme on G such that $G_{right} \le \mathrm{Aut}(\mathcal{C})$. Any scheme satisfying the latter condition is called a *Cayley scheme* on G. In fact, the above correspondence induces a bijection between the S-rings on G and the Cayley schemes on G that preserves the natural partial orders on these sets. Obviously, $\mathcal{R}^* = R_G(\mathcal{S}^*)$ and $\mathcal{E} = R_G(\mathcal{H})$. Moreover,

$$\mathrm{Aut}(\mathcal{C}) = \mathrm{Aut}(\mathcal{A})\, G_{right} \tag{26}$$

where $\mathrm{Aut}(\mathcal{A}) = \mathrm{Aut}(\mathcal{C})_v$ with $v = 1_G$.

Theorem 7.2 *Let $\mathcal{A}$ be an S-ring over a group G and H a normal $\mathcal{A}$-subgroup of G. Then* $\mathrm{Aut}(\mathcal{A})$ *normalizes the group $\langle \mathrm{Aut}(\mathcal{A}'), H' \rangle$ where $\mathcal{A}'$ is the S-ring over G generated by $\mathcal{A}$ and the cosets of G by H, and H' is the subgroup of the group G_{right} corresponding to the multiplications by the elements of H.*

Proof. Let $\mathcal{C}$ and $\mathcal{C}'$ be the Cayley schemes over the group G corresponding to the S-rings $\mathcal{A}$ and $\mathcal{A}'$ respectively. Then $\mathcal{C}' = [\mathcal{C}, \mathcal{R}]$ where $\mathcal{R} = \{R_G(C) : \ C \in G/H\}$ (see (25)). Let us show that

$$\mathcal{C}_E = (\mathcal{C}')_E \tag{27}$$

where $E = R_G(H)$. Indeed, since obviously $\Delta(C)$ is a relation of the scheme $\mathcal{C}_E$, so is the relation $R_G(C)$ for all $C \in G/H$. This implies that $\mathcal{R} \subset \mathcal{R}^*(\mathcal{C}_E)$ and hence $(\mathcal{C}')_E \le \mathcal{C}_E$. Since the converse inclusion is clear, equality (27) is proved. Next, we have

$$\mathrm{Aut}((\mathcal{C}')_E) = \mathrm{Aut}(\mathcal{A}')H'. \tag{28}$$

Indeed, by definition $\mathrm{Aut}(\mathcal{C}') = \mathrm{Aut}(\mathcal{A}')G_{right}$. Besides, due to the normality of H we have $(G_{right})_E = H'$. Thus from the obvious equality $\mathrm{Aut}(\mathcal{A}')_E = \mathrm{Aut}(\mathcal{A}')$ it follows that

$$\mathrm{Aut}((\mathcal{C}')_E) = \mathrm{Aut}(\mathcal{C}')_E = (\mathrm{Aut}(\mathcal{A}')G_{right})_E = \mathrm{Aut}(\mathcal{A}')(G_{right})_E = \mathrm{Aut}(\mathcal{A}')H'$$

whence (28) follows.

Since $H \in \mathcal{H}(\mathcal{A})$, we have $E \in \mathcal{E}(\mathcal{C})$. So from (24) it follows that $\mathrm{Aut}(\mathcal{C}_E)$ is a normal subgroup of $\mathrm{Aut}(\mathcal{C})$. This implies that the group $\mathrm{Aut}(\mathcal{A})$ normalizes $\mathrm{Aut}(\mathcal{C}_E)$. However $\mathrm{Aut}(\mathcal{C}_E) = \mathrm{Aut}((\mathcal{C}')_E) = \mathrm{Aut}(\mathcal{A}')H'$ by (27) and (28), and we are done.■

[4] If $C = H$, then the normality of H is not necessary.

References

[1] A. E. Brouwer, A. M. Cohen, A. Neumaier, *Distance-regular graphs*, Springer, Berlin, 1989.

[2] J. D. Dixon, B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics, No. 163, Springer-Verlag New York, 1996.

[3] R. W. Goldbach, H. L. Claasen, *Cyclotomic schemes over finite rings*, Indag. Math. (N.S.), **3** (1992), 301–312.

[4] R. McConnel, *Pseudo-ordered polynomials over a finite field*, Acta Arith., **8** (1963), 127–151.

[5] B. R. McDonald, *Finite rings with identity*, Pure and Applied Mathematics, Vol. 28, Marcel Dekker Inc., New York, 1974.

[6] T. Ito, A. Munemasa, M. Yamada, *Amorphous association schemes over the Galois rings of characteristic* 4, European J. Combin., **12** (1991), 513–526.

[7] S. Evdokimov, I. Ponomarenko, *Characterization of cyclotomic schemes and normal Schur rings over a cyclic group*, Algebra and Analysis, **14** (2002), 2, 11–55. (English translation in St. Petersburg Math. J., **14** (2003), no. 2, 189–221.)

[8] K. H. Leung, S. H. Man, *On Schur Rings over Cyclic Groups, II*, J. Algebra, **183** (1996), 273–285.

[9] Z.-X. Wan, *Lectures on finite fields and Galois rings*, World Scientific Publishing Co., Inc., River Edge, NJ, 2003.

[10] H. Wielandt, *Finite permutation groups*, Academic press, New York - London, 1964.

[11] H. Wielandt, *Permutation groups through invariant relations and invariant functions*, Lect. Notes Dept. Math. Ohio St. Univ., Columbus, 1969.